Interested in learning more about security?

SANS Institute InfoSec Reading Room

Endpoint Security Justification and Establishment

As the information security officer at a prominent utilities organization, I witnessed first hand the pitfalls of providing network security only at the network perimeter, the false sense of security, and the potential monetary, regulatory and credibility consequences this traditional solution provides. After discovering the problem to be a prevalent one, and concluding that the situation would not go away, persuaded the CIO, IT management, and IT department representatives to allow me to research and provide a tactica...

Endpoint Security
Justification and Establishment

Written by Samuel Ho
Date: July 16, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b (amended August 29, 2002)

Table of Content

Abstract

As the information security officer at a prominent utilities organization, I witnessed first hand the pitfalls of providing network security only at the network perimeter, the false sense of security, and the potential monetary, regulatory and credibility consequences this traditional solution provides. After discovering the problem to be a prevalent one, and concluding that the situation would not go away, persuaded the CIO, IT management, and IT department representatives to allow me to research and provide a tactical and strategic solution. The goal of my 2 months research was to find the right solution to the problem. The industry terminology of the solution is called Endpoint Security. Endpoint Security extends the traditional security perimeter to network's edge device or end users device. End user devices are most commonly the workstations and laptops used to access a corporate network. Utilizing endpoint security vendor analysis and product evaluations, insightful presentations and communications with the CIO and IT management, I was able to obtain funding for this solution and pilot test with minimal user impact.

This case study takes you through one approach of performing a security baseline to establish a security posture, and moving from a non-security focused IT environment to a proactive security culture where security is a goal and becomes part of the process in any IT project. You will witness how this security posture establishment discovers a security void. This case study suggests a process for researching information in the endpoint security industry to evaluate, pilot, and select a vendor for a particular environment. Ultimately, this case study validates why security protection at the perimeter is not sufficient to protect today's mobile workforce.

Introduction

As a senior security consultant at a private professional services organization, I am on a multi-year assignment at a prominent utilities company. My role at the client organization is to be the information security officer. The client has never had personnel dedicated for IT security and currently, I am the only person in the company in this role.

My initial investigation of the client infrastructure uncovered the lack of security model, security policy and procedure, and IT security focus in general. Due to the lack of proactive security presence in the past, the infrastructure had no security model and IT projects and deployment had little security focus. Only in the last few years, especially after the events of September 11, 2001 has IT security been given a higher priority in organizations across the nation. Wide acceptance of the internet, new security threats, and the new mobility paradigm using wireless and high speed corporate network access are also factors in IT Security moving to a higher priority.

Background

The client outsourced their network services department to our professional services organization. We had a team of 3 network consultants running the network services department. I began my assignment in 2001 replacing the lead network consultant who was transitioning out of the account. In this role, I helped improved the stability of the network, demonstrated value-add and return on investment (ROI) for proposed network projects, and assisted IT senior management in annual budget forecasting.

Network Stability

The network architecture was relatively flat with a 2 tier design. The 2 core switches and routers were centralized at the company's headquarters. Headquarters was made up of a campus of seven buildings, each of which housed at least one switch, to which all user equipment was connected. The building switches were all connected via multi-mode fiber to Building 5, where the computer room and the two campus core switches were located. Each core switch contained a router blade. WAN routers were located at headquarters, and at each of the remote sites. The core routers used were Cisco's Multilayer Switch Feature Card (MSFC) or router blades installed in the core switches. As a team, we added redundancy to campus building connections by multi-homing

these connections to both core switches, and we implemented redundant connections to critical servers and critical application servers in the server farm. The redundant server connections were configured for active-passive mode, according to the server configuration standard. Also, we hard coded all server-to-switch connections to prevent known problems with Auto/Auto interface problems, such as flapping.

The Wide Area Network originally incorporated Frame Relay, but was later replaced with a fully-meshed Point-to-Point VPN technology (which is discussed later). To assure network stability and maximum uptime we implemented Dial-on-Demand Routing (DDR) or stand-by connections for backup, using a completely separate technology called Integrated Services Digital Network or ISDN. DDR automatically brings up the ISDN backup link(s) whenever the primary route becomes unavailable, and there are data packets that need to be sent to a remote site. DDR also automatically brings down the ISDN link(s) after five minutes of inactivity. DDR provides an ISDN backup link within seconds of the primary link's failure. The primary link failure is detected by the loss of the route mapping (using EIGRP) in the routers route table. This happens dynamically by nature of the Cisco's EIGRP routing protocol. At this point, the standby connection uses the ISDN protocol to initiate a connection at the remote site to headquarter. Within seconds, the standby connection gets established and traffic can traverse through it. When the primary link is restored, the primary route is generated in the route table. By virtue of Cisco's EIGRP, traffic then traverse back through this primary link and the standby DDR ISDN connection automatically terminates after five minutes of inactivity. Thus, when the primary link is restored, the primary route reappears dynamically in the WAN router, and data traffic then traverses back through the primary link.

The network team performed a top down re-architecture of the company's internet perimeter in favor of redundancy, manageability, and security. We replaced the perimeter stand alone Cisco PIX firewall with dual Checkpoint Stateful Inspection solution. The new firewall incorporated a distributed design where the management server is separate from the firewall enforcement appliance. This distributed platform offered a greatly enhanced security solution than what was previously in placed. It also discouraged configuration mistakes facilitated firewall administration adds, moves and changes. The Checkpoint solution offered superior management and architecture options that were superior to the Cisco PIX appliance solution at that time. Redundancy won over the standalone PIX solution. To implement this, we ran the Checkpoint application running on two Nokia hardware appliances. We implemented Nokia VRRP configured in active/passive mode for redundancy and automatic fail-over. With the core of the perimeter now fully redundant, we replaced the single connections to each Demilitarized zone or DMZ with redundant ones to the new dual firewall.

Budget limitations must always be weighed against network uptime. Inevitably, for more uptime, more money must be dedicated to the network infrastructure. Due to budget imitations, we acknowledged that network outages may still occur. Failures might occur on the hardware, software, circuit, or configuration levels. Since we could not completely prevent network failures, we needed to concentrate on mean-time-to-recovery (MTTR). To provide access to remote network devices, I implemented an out-of-band-management (OOB) solution. This solution allowed administrators to remotely access, control and manage network devices through analog lines. Administrators could then access a device's console screen as if they were in directly connected to the device. This solution comes in handy when the administrator is unable to telnet to the device for any reason. When troubleshooting, it allows the administrator to get to the heart of the problem and thus, decreases MTTR.

Value Add and Return on Investment on Proposed Network Projects

The network team performed many cost analysis and return-on-investment (ROI) calculations for network projects. Although ISDN does not provide nearly the same bandwidth that Frame Relay or Point-to-Point VPN connections can provide, choosing to go with ISDN for remote standby connection proved to be a huge value-add. The cost for this solution is negligible – less than $100 per month per site in recurring costs. ISDN is a pay-as-you-use service, much like your home phone service. There is a basic monthly service fee, but only when the ISDN is activated are you charged a per minute usage fee based upon published local and/or long distance rates (this usage fee can be recovered for outages caused by the circuit from your primary circuit provider if you manage the service level agreement appropriately).

As another cost saving project, I spear-headed the initial pilot and deployment of an Internet-based Virtual Private Networks or VPN WAN to replace the existing frame relay WAN. Cost analysis showed a six-month ROI for the one-time VPN equipment investment required. The company realized an increase in bandwidth at all remote sites of between 300 and 500% for the same circuit costs! Of course VPN circuits are less ideal for delay and jitter sensitive applications (like Voice over IP) but after baselining the network, we found that these applications were not being used. The VPN WAN design also incorporated split-tunneling, which provided all remote sites with direct access to the internet, relieving the headquarters site of the burden of playing middle-man for all of the remote site's Internet traffic, both incoming and outgoing. The performance result was clearly more efficient and much better for end users. As for security, internal data traveling between company sites, including EIGRP router updates, is automatically encrypted using the triple-DES and IPSec protocols. EIGRP router

updates through the IPSec tunnel were possible with the usage of Cisco's GRE protocol.

Annual Budget Forecasting

Proper financial management is critical in every department. The IT services department is no different. Managing the IT project budget requires due diligence in project forecasting and funding requirements. Network Services maintains a list of network projects. They are continually ranked and re-ranked in order of importance. During the budget cycle, we worked with vendors for actual project quotes. The project quotes and rankings allow us to ensure we do not go over budget and that high ranking projects get appropriate funding. I reviewed project ranking and budget forecast through out the year. Often unexpected unbudgeted projects arise. Lower priority projects are often sacrificed to fund these unexpected projects. At the end of the year, IT does not exceed its budget forecasts and it maintains a good reputation with the finance department.

Roles and Responsibilities

I was responsible for the network projects outlined from inception, through business analysis, vendor evaluation and selection to design, implementation and maintenance. As part of the network team, we took the divide-and-conquer approach. My teammates performed parallel tasks on similar as well as other projects. The goals and processes of our projects were the same. The goals were to provide network stability and redundancy, demonstrate value-add and provide appropriate returns on investment (ROI) for proposed network projects, and assist senior management in annual budget forecasting.

In the beginning of 2002, my network role expanded to be more information technology security focused. In the summer of 2002, I was designated the Information Security Officer where my primary responsibility was to support IT security at an operational and business process level. This dedicated security position is a first for the company. The company is medium-sized with 800 + employees. Part of my responsibility now is to work with the senior management and the CIO directly to ensure compliance for federal and state IT security mandates, and security issues and projects. Operationally, I architecture, implement, and maintain network and application level security systems. With other IT projects and issues, I play the role of the Security Matter Expert (SME) where I provide security awareness and "shine a security light" onto the picture. At the same time, I make sure that corporate security policies and procedures are followed and kept up to date. The past IT culture was not security focused, I had to define for management the roles and responsibilities of the Information

Security Officer, tactfully persuade and encourage administrators to be security mindful and consider security a high priority in IT operations, processes, and projects.

Security Posture

When I first started the security position, I realized that security incident management was reactively pursued, security infrastructure was very limited, and formal policy and procedure structures were nearly non-existent. I proceeded to perform a security baseline assessment of these areas in order to establish a Security Posture. Afterward, I worked to continually improve them.

Security Incident Management Posture

Formal process forms were limited and not up to date. As a result, existing forms such as add, move, and change control forms were often not used by the IT staff. This process contributed to a lack of documentations. As a result, groups within IT worked in a vacuum where one group was not aware of another group's activities. Consequently, one group may spend numerous hours troubleshooting a problem that may have been easily avoided through better communications and documentation. Often, when a service or application breaks, the user contacts the helpdesk. The helpdesk contacts the Application or the Server teams. The Application or Server group, not knowing what changes were made to the network, might spent hours checking their systems to locate the culprit of the application or service malfunction.

The forms below existed but they were not up to date and were seldom used. A thorough review of them was performed and changes were made where necessary.

- Basic Network Services Design Change Worksheet
- Problem/Change Control Form
- Incident Report Form
- Project Work Request

For IT Security process improvement and incident management, the following forms were created.

- Firewall Change Control – For firewall adds, moves, or changes.
- Network Change Control – For network adds, moves, or changes.
- Static Ip Address Control – For static ip address requests and allocation.

- VPN Site-to-Site Request Form - For business partner virtual private network establishment requests.

These forms were used extensively once they were created and published to the IT staffs. In fact, these forms encouraged the server supervisor to create a number of similar forms specific to their group:

- Server Group Services Change Request Form
- DNS Request Form

The forms enable IT groups to be aware of when something is going to be done to systems or the network. This expedites problem resolution and troubleshooting, avoids duplication of effort, and facilitates communications between IT groups. During post mortems, records of these forms even help to facilitate discussions.

Security Infrastructure Posture

For simplicity, the security infrastructure was broken down to several areas: Physical security, email security, anti-virus, perimeter security, remote access VPN, remote office VPN, and IT audits. This break down allows me to get a perspective on the many facets of the company's IT Security. I have decided to research the baseline in each of these areas and where appropriate, provide quick security fixes and recommendations. The security concerns that take longer to resolve are noted for future security projects.

Physical Security

Physical security consists of badge access control for and employees and contractors. This area is currently managed by the company's Facilities department. This function and process has not been changed.

Email Security and Anti-Virus

Two email security issues needed to be addressed, SPAM and anti-virus management.

Initially, we had no central corporate email gateway or system. Our only defense against viruses and worms was the McAfee® VirusScan anti-virus program used on personal computers and laptops. This anti-virus software was part of the

standard build for new personal computers and laptops. However, anti-virus software is not effective in guarding against new viruses unless the anti-virus software is kept up to date. We discovered that after the newly built systems were released to employees and authorized contractors, there was no effective way to ensure that the anti-virus software was enabled and the signature file was being kept up to date. Also, anti-virus software defends against all viruses entering a system, not just viruses that come through email. This type of anti-virus software was ineffective in defending against SPAMS on corporate email accounts as a whole. The inability to manage anti-viruses is noted as something to resolve later.

Working collaboratively with the email administrator, we looked for a corporate gateway email filter system that best fits in the company's environment. We narrowed the selection to two best-of-breed vendors with very different design approaches.

The first product we evaluated was Trend's Micro's InterScan VirusWall.[1] The product's features, capabilities and functionalities seemed impressive. [2]

The design approach for this product is that the email filter is to be implemented and managed in-house. One of the reasons this in-house product may be suitable to the company's environment is their partnership relationship with Checkpoint. This partnership is called Open Platform for Secure Enterprise Connectivity or OPSEC.[3] OPSEC is a policy-based management framework for best-of-breed security products.

Because Checkpoint is also our Firewall vendor, I found it easy to configure the firewall to work with the InterScan Virus Wall server during the evaluation phase. In addition to SMTP or email filtering, it is relatively easy to configure HTTP and FTP filters between the InterScan Virus Wall application and the Checkpoint firewall. HTTP and FTP filters are included with the InterScan VirusWall application. We know these features will work because of the OPSEC relationship; that is both vendors tested the interoperability successfully. Because of the successful evaluation of the InterScan VirusWall application and the OPSEC benefits mentioned, we decided to go with this in-house solution. This filter solution proved to be 75% effective. The InterScan VirusWall gateway

[1] Trend Micro Incorporated. InterScan VirusWall Product Overview. 28 June 2004 <http://www.trendmicro.com/en/products/gateway/isvw/evaluate/overview.htm>.

[2] Trend Micro Incorporated. InterScan VirusWall Features. 28 June 2004 <http://www.trendmicro.com/en/products/gateway/isvw/evaluate/features.htm>.

[3] Check Point Software Technologies Ltd.. October 5, 1998. Check Point Software Technologies And Trend Micro Team To Combat Internet Gateway Security Threats. 28 June 2004 <http://www.checkpoint.com/press/1998/trendmicro100598.html>.

blocked 75% of all inbound SPAM emails after fine tuning the application for the first 3 months of deployment. Unfortunately, it was difficult to do better than that because administering and fine turning the InterScan VirusWall application for one email administrator became a daunting task, especially when you have 500 plus end users breathing down your neck about that 25% SPAM and some users complained about the InterScan VirusWall blocking legitimate email. When a legitimate email was blocked, the email administrator would have to release or white-list (terminology and definition) that particular email or sender. All of the issues experienced during and after the deployment made us reconsider alternate email filter solutions.

The alternate solution we explored was to outsource the email filter functionality. This solution presented one particular security risks however. The set up requires us to provide the company's MX record to the outsource server. This resulted in all company email (inbound and or outbound) going through the screening server. This solution is not suited for every organization and every organization needs to consider their own policy and procedure for management of their intellectual property, sensitive information, and company data (like email). We declared that emails should not contain sensitive company data and should not be a medium used to distribute intellectual property without transient or encryption security.

The outsource solution we went with was Message Screen by IntilliReach.[4] The benefits of the Message Screen product over the InterScan VirusWall were exactly what the company needed.[5] In particular, these determination factors are:

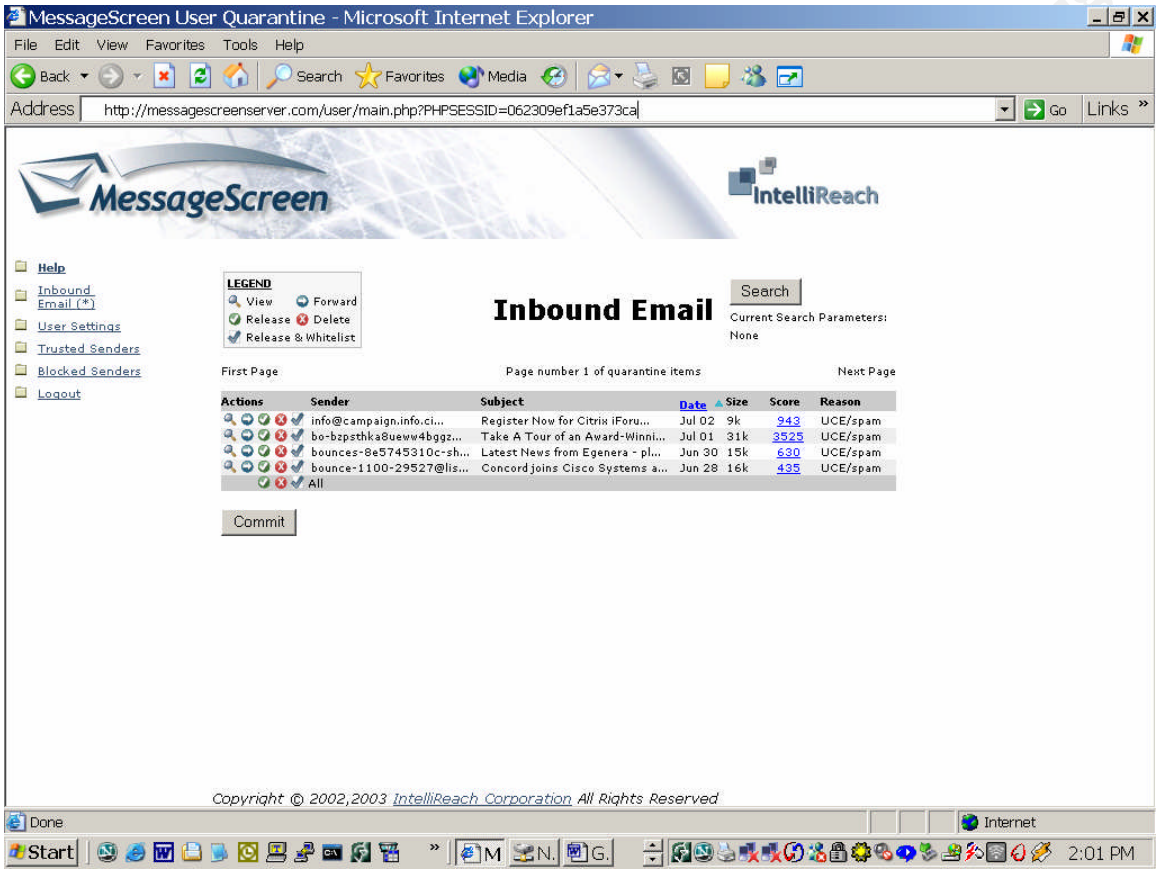
- SPAM Blocking Effectiveness – IntilleReach claims that their solution "blocks over 98% of SPAMs and explicit content while producing virtually zero false positives."[6]
- Administration off load and mitigation - For the email administrator there is no need to implement, support and maintain additional hardware and software.
- User Interface Filter management - End users have the ability to manage and custom their own email account (through web interface). They can access their SPAM filter setup and decide which email, sender, or domain name are legitimate and which ones get blocked. IntilliReach calls this feature, "Enhanced User Controls and End-User Quarantine."[7]

[4] IntelliReach Corporation Website. Email Management Solutions. 28 June 2004. <http://www.intellireach.com/index.htm>.
[5] IntilleReach Corporation. The MessageScreen Advantage. 28 June 2004 <http://www.intellireach.com/products/messagescreen/MS_advantage.htm>.
[6] IntilleReach Corporation. MessageScreen Product Description. 28 June 2004 <http://www.intellireach.com/products/messagescreen/index.htm>.
[7] IntilleReach Corporation. The MessageScreen Advantage. 2 July 2004 <http://www.intellireach.com/products/messagescreen/MS_advantage.htm>.

After deploying the IntilleReach solution, the above benefits were realized. The SPAM blocking effectiveness was remarkable. Within the first few hours of deployment, Message Screen blocked 20 to 25 percent more than the InterScan VirusWall. This statistic was verified by deploying the Message Screen solution behind the InterScan VirusWall solution.

The appliance, hardware and software is owned and maintained by IntilleReach. Besides opening some TCP and UDP ports at the firewall in the initial deployment, this outsource solution requires minimal support from our Email Administrator.

The user interface is truly user friendly. Changes can be made by simply committing to which emails to forward, release, or delete. Here's a picture of the user interface for my account:



The Perimeter

At the perimeter, not much is needed to improve here since I was part of the team that replaced the standalone firewall with the redundant firewall systems. To improve the performance and efficiency of the firewall systems, I consolidated and removed redundant security policy rules, and moved the most used rules to the beginning of the configurations.

Remote Access VPN

Encryption should be used when accessing company resources from or through the Internet. One type of internet based access is called virtual private network or VPN. Our company has two categories for VPN, Remote Access and Remote Office Site-to-Site.

The company's remote access VPN solution was found to be relatively secured but certain cyber security risks were discovered. These risks could potentially cause compromises to the corporate network and are considered high. The VPN solution uses IPSec protocol with 3DES encryption. The 3DES encryption protocol has been the IEEE standard until end of 2003. Beginning 2004, the IEEE committee endorsed AES as an encryption standard. Our remote access VPN solution was configured to support 3DES. An upgrade to the VPN gateway would be needed to support AES protocol. However, this gateway has reached its hardware limitation and can not be upgraded. In the future, we will need to replace the VPN gateway in order to roll out AES. Another security issue discovered was the lack of restriction to the company's network resources. For example, there was no way to restrict employees from accessing the company's network from an unauthorized computer, like their personal computer. Because employees have access to the VPN client software, they can install it on any system and with their authorized network sign-on account, they can obtain network access. This is a huge security concern because it represents a network entry through the backdoor with systems that are virtually unknown to IT administrators; thus viruses and malicious codes can be introduced into the network this way. This finding was noted and as an action item, a permanent solution is needed in the near future.

Remote Office VPN

I performed the pilot and initial deployment of the Site-to-Site VPN between corporate and remote offices. As an Information Security Officer, I reviewed the configurations again; this time with more of a security mindset. The VPN parameter's used are:

IKE Parameters
IKE Proposal: IKE-3DES-SHA1-DH2 (1024-bit)

IPSec Parameters
Authentication Algorithm: ESP/SHA1/HMAC-128
Encryption Algorithm: 3-DES-168

The conclusion for the security of the remote office site-to-site VPN was that they are relatively secured. In the future, an upgrade of the encryption algorithm from 3DES-168 to AES is needed. The hardware and software existed are capable of supporting AES already.

IT Audits

Two types of IT audits existed. The company arranged one of the big five accounting firms to perform regular annual IT audits. This audit is high level and the process consists of interviewing IT management and administrators regarding various IT configurations, including IT security. The deliverable is a presentation to IT Management, including the CIO, of their findings accompanied with recommendations. The general feedback I received about this type of audit was that they were not useful. I saw a copy of their presentation and I agreed that improvements can be made so these audits are more effective and practical.

The second type of IT audit is a Security Assessment and Penetration Test performed by a third party Professional Services company. This type of IT audit is the first for the company and it is not certain that this service will occur again because of the high cost. I reviewed the security assessment and penetration test deliverables. I was impressed! The documents were thorough and insightful with specific security findings and recommendations for problem resolution. In my experience, most recommendations in these types of deliverable reports are not completely implemented or carried through. Companies spent countless

monies for Professional Services but only have stacks of reports or documents to show for. This can potentially happen to us.

I decided to carry out the problem resolution recommendations. With these documents on hand, I was more empowered to access system configurations from other IT groups. This turned out to be an effective way for me to acquire an overall security configuration on systems and develop a security baseline. By working with administrators to upgrade, harden, enhance and improve configurations on their respective systems and applications, we improved the security for:

- The UNIX Servers
- Unix Production Servers
- Unix Web Servers
- DNS Systems
- BIND Servers
- The Microsoft Servers
- Microsoft Web Servers
- Microsoft Production Servers
- Applications for PeopleSoft, Sybase, DB2, and Documentum
- Database for Sybase, DB2, and MS SQL
- The Perimeter Devices
- Firewall Systems
- Co-location Connections and Devices
- Remote Access Devices
- Remote Office Devices
- Networking Devices

To ensure that the above systems are secure and up to date with the latest fixes against new vulnerabilities, I incorporated regular and irregular penetration tests. These tests consist of port and system scans from inside and outside our network on the above systems and applications into the security process. Regular monthly scans are important to ensure product updates, vulnerability checks and fixes, product version releases and accesses are met. Also, regular scans ensure compliance to notification of critically released advisories. These scans are not intrusive and when carefully performed, should never unintentionally bring down systems and applications. Irregular scans are critical to ensure proper system configurations and to instill a security mindset at all times.

Security Policy and Procedure

The Security Assessment called out a need for a formal security policy and procedure. None existed when I first took up the role. This is an important gap that needs to be filled right away if the company was serious about being IT Secured focused. A formal security policy and procedure is the first step to change a non-security focused culture. If done properly, it brings security issues to the table, educates users about IT Security, and gets management on board with the security policy and procedure.

The term policy and procedure are often misunderstood. According to SANS Institute, this is how they are defined:

> "A policy is typically a document that outlines specific requirements or rules that must be met. A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice."[8]

SANS defined guideline as synonymous to procedure. SANS website states the above definition and also has policy and procedure templates.[9]

These templates are just samples. Every organization should work with their Management and tailor them to meet their company needs. For us, we followed the same policy and procedure definition. Instead of the word Policy, we called it Capstone because practically, a policy is the top set of specific procedures. Also, our users and management can relate to the word Capstone better.

Using the SANS policy and procedure as templates, I published the following procedures on the company's internal website.

> **User Account Procedure** – This procedure is meant to prevent users from sharing user accounts and passwords on the network.
>
> **Password Procedure** – This Procedure is intended to ensure security regarding user accounts and network access. It will force users to create passwords that are not easily compromised thus making it harder for a person to guess or decipher the password for misuse.

[8] The SANS™ Institute. The SANS Security Policy Project. 2002-2004. Need an Example Policy or Template? 2 July 2004. <http://www.sans.org/resources/policies/>.
[9] The SANS™ Institute. The SANS Security Policy Project. 2002-2004. Is it a Policy, a Standard or a Guideline? 6 July 2004. <http://www.sans.org/resources/policies/>.

Remote Access Procedure – This procedure describes appropriate usage of the network from remote locations. This includes accessing the network through dial-in connections and any other connection such as DSL, Cable Modems, etc..

Virtual Private Network (VPN) Procedure – The VPN procedure describes appropriate usage and security measures regarding accessing the network via a VPN connection. These connections can be established through any remote connection to the Internet.

Analog/ISDN Line Security Procedure – Analog and ISDN lines entering a network are often overlooked entry point into a computer network. This procedure details how these lines should be deployed and properly used to maintain the best security.

Wireless Communications Procedure – As wireless technology and devices become more readily available and also become easier to implement the security with these devices becomes more of a concern. It is important to implement a wireless procedure to outline the appropriate usage of these devices on the network. If configured or used improperly these devices create an open door to users who may have bad intent.

Acceptable Encryption Procedure – This procedure will detail the specifications required to ensure that any encrypted data within the network is of the most secure nature. It also describes restrictions regarding export of certain types of encryption outside the United States.

Audit Procedure – The ability for the network security group to audit computers for possible security flaws is important in keeping servers and other computers safe from attack. This procedure mandates that the team have access to audit all machines to identify security flaws.

DMZ Lab Security Procedure – This procedure outlines the requirements of placing computers or other devices on the DMZ Lab. The intent is to make sure that these devices are not easily open to attack from outside the network.

Extranet Procedure – This procedure will detail restrictions in how we will create extranet connections with business partners. All connections into the network to be shared with outside parties are serious security risks.

Internet DMZ Procedure – This procedure outlines the requirements of placing computers or other devices on the Internet demilitarize zone, DMZ. The intent is to make sure that these devices are not easily open to attack from outside the network.

Lab Anti-Virus Procedure – This procedure requires that all machines in labs within the network are required to have Anti-Virus software installed. This eliminates the threat that viruses could be spread to the network from computers in a lab that may be running non-production or non-tested software.

Contractor PC Audit Procedure - This procedure provides the authority for members of the information security team and Helpdesk to conduct a security audit on contractor workstations, sister company workstations, and employee personal computers (PC). This procedure requires all non-company systems get certified for access to the network.

As the owner of these procedures and IT Capstone, I ensure these documents are updated and posted in the company's internal website.

Proactive Security Management

By performing a security baseline, I have a well defined security posture of the environment I am responsible for. I was able to implement some urgent security fixes; like IT Security, capstone, procedures, process controls and forms, to quickly improve the security posture. This can be done by utilizing the resources, like IT Security Assessment and Penetration Tests, already available to me. We resolved an urgent security concern by implementing a manageable anti-virus solution. The next step is to continue to turn the security environment from one that is all reactive to more a proactive state.

Intrusion Detection Systems

The first proactive security system I deployed is a network intrusion detection system (NIDS). NIDS' are expensive so I recommend a phase approach deployment until funding can be justified for a network wide implementation. After weighing the risk tolerance level and generating a cost analysis, we decided to deploy NIDS first at the perimeter. This approach is recommended for any environment looking to test a NIDS solution. After this initial deployment, the risk tolerance can be reevaluated for NIDS to be deployed elsewhere in the network.

The NIDS solution we went with is Internet Security Systems' (ISS) RealSecure. Their solution operates in both signature and behavioral based. Both these operations are needed for effective NIDS these days. ISS offers a cost effective

appliance solution, Proventia Intrusion Prevention.[10] Their RealSecure software solution can only be deployed on a third party appliances, like a Nokia 360, which can cost you another $7,000.00 (the includes Nokia's Operating System, IPSO). In the initial set-up, I recommend to only turn on the intrusion detection function. If not done correctly, NIDS can generate many false positives and the intrusion prevention can kill legitimate sessions. NIDS logs are huge so get as much hard drive space as possible. Making sense out of the logs can be extremely time consuming so managing false positives and configuring what to log cautiously. Turn on intrusion prevention only after you get use to the intrusion detection function.

Another proactive system deployed in the network is hosts based intrusion detection systems (HIDS). In our environment, the server team owns the implementation of this solution. My role is to offer security guidance in the vendor selection and deployment process, and ensure that the application does it job in meeting the security requirements. HIDS' are also expensive. If cost is an issue, scale down the initial deployment. I recommend getting limited agent licenses initially and deploy in critical systems only. The solution we went with is Security Manager[11] by NetIQ.

Endpoint Security

Most companies end proactive security management with the deployment of Intrusion Detection and Prevention. In a traditional network environment, where user mobility is limited or less frequent, this would suffice. In today's network environment, we have to provide and enforce proactive security further out to the network edge, like endpoint devices. The findings during the security baseline process are a prime reason for this company to adapt to this new security paradigm.

Security Findings Re-visited

During the security baseline and security posture establishment processes, recall that I discovered a few unresolved security issues. A summary of these security issues discovered are:

- Inability to manage anti-virus on computer workstations and laptops.
- Inability to certify anti-virus software while connecting to the network.

[10] Internet Security Systems. Proventia Intrusion Prevention Product Overview. 8 July 2004. <http://www.iss.net/products_services/enterprise_protection/proventia/g_series.php>.
[11] NetIQ Corporation. 1993 – 2004. Security Management Solution Overview. 8 July 2004. <http://www.netiq.com/solutions/security/default.asp>.

- Inability to ensure that anti-virus is updated.
- Restrict users from accessing the company's network resources from unauthorized computers.

Every year, I give a 'state of the company's cyber security' presentation to IT Manager, supervisors, and the CIO. During this year's presentation, I presented that the current security infrastructure is not secure enough to support a new network access medium as demanded by users, the security findings, the company's security model, and communicated IT security's weakest link, which needs immediate attention.

User Demand Service

Wireless is currently not an IT supported service. This is stated and published in the wireless security policy and procedure. This wireless access restriction is questioned and challenged more and more each year by the user community. No matter how often I explained to users about the insecurities of wireless access in our environment, the wireless convenience factor prompts them to ask for supporting this service. Some convenience factors include network access mobility and roaming, increase productivity, and wireless set-up simplicity.

Wireless Access Points (AP) can be bought at Fry's Electronics for less than $100. The simplicity of setting a wireless network is as easy as connecting APs into the company office network port and installing a wireless network interface card (WNIC). In fact, new laptops in the company come with standard built in WNICs. For these reasons, it is understandable that Wireless support is inevitable. I came to this conclusion after returning to work from last year's Christmas break. My wireless analyzer detected three campus wireless connections. I was able to track them down and retrieved these rogue wireless APs. I immediately sent out a reminder to the user community that company policy restricts wireless devices in campus and that wireless access is not supported. In the back of my mind, I knew this service has to be supported it sooner or later. If not, users will try to install rogue APs themselves.

In our environment, securing the wireless infrastructure is not a problem. We can deploy a secure wireless campus network with encryption. The core problem here is securing end devices, like laptops. These laptops are susceptible to port scans, malicious code injections and other cyber attacks while accessing from home or at public wireless network, like hotspots.

Security Model

For the IT Security Model discussion, I introduced Security as a defense in depth or multi-layered approach. This peel the onion security approach is common in the security community. Security professionals defend against attacks by guarding at every layer (like the OSI 7 layer) of the network.

Also, I presented the concept and usage of a security matrix rating. Like a baseball scorecard, this security matrix rates the individual elements in a company's IT infrastructure. The security matrix can be ultimately used by IT management to promote IT Security and justify funding for IT Security projects. For me and the company system administrators, this security matrix clearly demonstrates the relative security position within IT. This demonstration is shown on the total score of each IT category or application. The most area of improvement is at the category with the lowest score, which I called the weakest link.

Security Matrix Model (Sample):

Rating Scale (1-5):	Note:
1- No Security 2- Few Security 3- Half Security 4- Most Security 5- All Security	Weighting Criteria: Equal weight Total Score = 25% * (Security Infrastructure + Process + Management + Mitigation)

Category	Title	Weighting Criteria / Weighting Area				Total
		25%	25%	25%	25%	100%
		Security Infrastructure (Physical, Firewall, NIDS, HIDS, Architecture)	Process (Policy, Procedure, Audit)	Management (Monitoring & logs)	Mitigation (Encryption, Identity Management)	
Ways We Communicate	Internal:					
	Local Area Network (LAN)	4.5	4.25	4	4	4.1875
	Remote Sites LAN	4.5	4.25	3.75	3.5	4
	Remote Sites Wide Area Network (WAN)	4.75	4.5	4.25	4	4.375
	Wireless Local Area Network	1.5	3	1.5	1	1.75
	External:					
	Blackberry	4.25	4.5	4.25	4	4.25
	Business Partner	4.5	4.75	4.5	4.5	4.5625
	PDA	4.5	4.75	4.5	4	4.4375
	Remote Access Users	2	3.5	2	4	2.875
	Wireless Hotspot	1	1	1	1	1
	Communication Methods:					
	Email	4.75	4.5	4	4	4.3125
	Instant Messaging or IM	2	1.5	1	1	1.375
	Telephone	4.75	4.5	4.25	4.5	4.5
Critical Application	Critical Application in installed Servers:					
	Security Server	4.25	4.5	4	4.5	4.3125
	Dev Server	4.75	4.75	4	4.5	4.5
	Production Server	4.5	4.5	4.75	4.5	4.5625

The Security Matrix above shows the weakest links are Wireless Local Area Network, Wireless Hotspots, and Instant Messaging. A company's IT security is only as strong as their weakest link.

Endpoint Security Solution

A solution to resolve the company's weakest security link is with Endpoint Security. This solution is increasingly needed as indicated in this article, "Demand for Endpoint Security is Growing"[12]. When deploy properly, Endpoint Security solves the company's following security concerns:

- Inability to manage anti-virus on computer workstations and laptops.
- Inability to certify anti-virus software while connecting to the network.
- Inability to ensure that anti-virus is updated.
- Restrict users from accessing the company's network from unauthorized computers.
- Secure end devices against port scans, malicious code injections and other cyber attacks while accessing from home or a public wireless networks, like hotspots.
- Ensure security and integrity of Wireless Local Area Networks, PDAs, Wireless Hotspots, and Instant Messaging medium accesses.

After demonstrating the urgent need for an Endpoint Security solution and getting management's buy-in, the next task is to assist IT Management in identifying funding for this project, perform vendor analysis and evaluation, pilot and deployment.

Endpoint Security Funding

Identifying funding for this project turned out to be an easy task. The initial average quote received from Endpoint Security vendors averaged $50K. This is just for the license for our size company. I then created a simple ranking of approved security projects. This ranking puts priority levels of security projects in perspective for you and management.

Here is what my security project ranking look like:

[12] CSO online.com. Michael Rasmussen, Forrester®. 2004. Demand for Endpoint Security Growing. 6 July 2004 <http://www.csoonline.com/analyst/report2170.html>.

Security Services Project Ranking		
Rank	Projects	Cost Estimate
1	Endpoint Security	$50,000
2	Wireless LAN Investigation and Pilot Including Security	$20,000
3	Enhanced remote access	$20,000
4	Port Based Security Research and Pilot	$20,000
5	Enhanced Content Security	$15,000
6	Remote Site Firewall Upgrade	$40,000
7	Hardware Centralize Management	$15,000

Now, suggest to management to use funds from your lowest priority ranking projects. According to the ranking, initial funding for Endpoint Security project will come from Remote Site Firewall Upgrade and Hardware Centralize Management projects. The reason these projects can be put off is because Endpoint security solves an urgent security void while allowing IT to support new services like wireless. Remote Site Firewall Upgrade and Hardware Centralize Management are projects to enhance the efficiency of administrative support. Clearly, Endpoint Security project is more important.

Vendor analysis

At this point, you received management buy-in and have funding for the project. To find out vendors in the Endpoint Security field, I used the following sources:

- Conferences - Like the RSA conference.[13] The opportunity to meet vendors face-to-face and talking to other security professional about their Endpoint Security experiences is invaluable.
- Security trade magazines – Like Network World.[14] You can get a wealth of technical and vendor information by doing a search for "endpoint security" at security trade magazine websites.
- Search Engine – I used google.com. A search for "endpoint security" here resulted in some of the vendors below. [15]

[13] RSA Conference Portal. Conference Portal website. 9 July 2004. <http://www.rsaconference.com/conf_portal.html>.
[14] Network World Fusion. Company website. 9 July 2004. <http://www.nwfusion.com/>.
[15] Google Search Engine. 2004 Google. Search Engine portal. 10 July 2004. <http://www.google.com/search?hl=en&ie=UTF-8&q=endpoint+security>.

Specific endpoint security product information can be found in the respective company website below.

Endpoint Security Vendor Analysis		
Vendors	**Solution Product Offering**	**Company Product Website**
Checkpoint	VPN-1 SecureClient	http://www.checkpoint.com/products/vpn-1_clients/index.html[16]
Cisco	Cisco Security Agent (CSA)	http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html[17]
Sygate	Sygate Secure Enterprise	http://www.sygate.com/products/sygate-secure-enterprise.htm[18]
Zone Labs*	Zone Labs Integrity	http://www.zonelabs.com/store/content/company/corpsales/intOverview.jsp;jsessionid=As1jI5ThbQawT6VgDhtjAcq2mk25pvAQk8qNFu3e11YsHCfabErE!-30283316!-1062696905!7551!7552!-2012896460!-1062696904!7551!7552[19]
Microsoft	Microsoft Script Solution**	http://msdn.microsoft.com/library/default.asp?url=/downloads/list/webdev.asp[20]
Note: *Zone Labs was bought by checkpoint in 12/15/03.[21] **Microsoft Script Solution - I did not find a specific enterprise class product offering on Microsoft's website and from talking to the local Microsoft SE. The endpoint solution offered using their MS Scripting language.		

During the selection process, we were able to quickly weave out some vendors. The Microsoft's scripting solution was not appropriate for our enterprise environment. Because of the nature of a scripting solution, it would be too time consuming to manage and deploy such a solution.

[16] Check Point Software Technologies, Ltd.. Endpoint security solution. VPN-1 Secure Client. 10 July 2004. <http://www.checkpoint.com/products/vpn-1_clients/index.html>.
[17] Cisco Systems, Inc.. 1992-2004 Cisco Security Agent Introduction. 10 July 2004. <http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html>.
[18] Sygate Inc.. 2004. Sygate Secure Enterprise. 10 July 2004. <http://www.sygate.com/products/sygate-secure-enterprise.htm>.
[19] Zone Labs Inc.. 1999 – 2004. Zone Labs Integrity Enterprise Endpoint Security. 10 July 2004. <http://www.zonelabs.com/store/content/company/corpsales/intOverview.jsp;jsessionid=As1jI5ThbQawT6VgDhtjAcq2mk25pvAQk8qNFu3e11YsHCfabErE!-30283316!-1062696905!7551!7552!-2012896460!-1062696904!7551!7552>.
[20] Microsoft Corporation. 2004. MSDN Library. 11 July 2004. <http://msdn.microsoft.com/library/default.asp?url=/downloads/list/webdev.asp>.
[21] Network World Fusion. Tim Greene, IDG News Service, 15 December 2003. Check Point buys Zone to bolster endpoint security. 11 July 2004. <http://www.nwfusion.com/net.worker/news/2003/1215checkzone.html>.

The Cisco's CSA solution looked promising. Unfortunately, this solution is too new. Their solution is a conglomerate of many acquired security solutions, including the technology purchased from Okena.[22] The concern with this solution is the effective integration process and product stability between Okena's technology and Cisco's security technologies. Okena technology is a good host based intrusion detection and prevention product though.

The Checkpoint VPN-1 Secure Client solution was also eliminated. We invited Checkpoint's System Engineer (SE) to discuss their endpoint solution product offering. One area of concern was that their solution needs an additional third party application to certify anti-virus software releases and versions. I also had reservation about the future of Secure Client with the recent acquisition of Zone Labs.

Finally, Sygate and Zone Labs were the top two vendors selected. Checkpoint's acquisition of Zone Labs was recent and both company SEs thought that treating the two endpoint products separately was the way to go.

Vendor Evaluation

Both Sygate and Zone Labs have best of breed endpoint security products. Both solutions have similar and distinct features. Sygate uses a pull technology where end devices pull for security policy updates. Zone Labs uses push technology where their Integrity Server pushes security policies to endpoint devices. We invited both Sygate and Zone Labs companies for evaluation.

Evaluation and Pilot Phase

Entering the evaluation phase, I have to ask myself what is the goal of the evaluation and what am I trying to achieve after evaluating and testing their products. Specifically, I seek answers to the following questions:

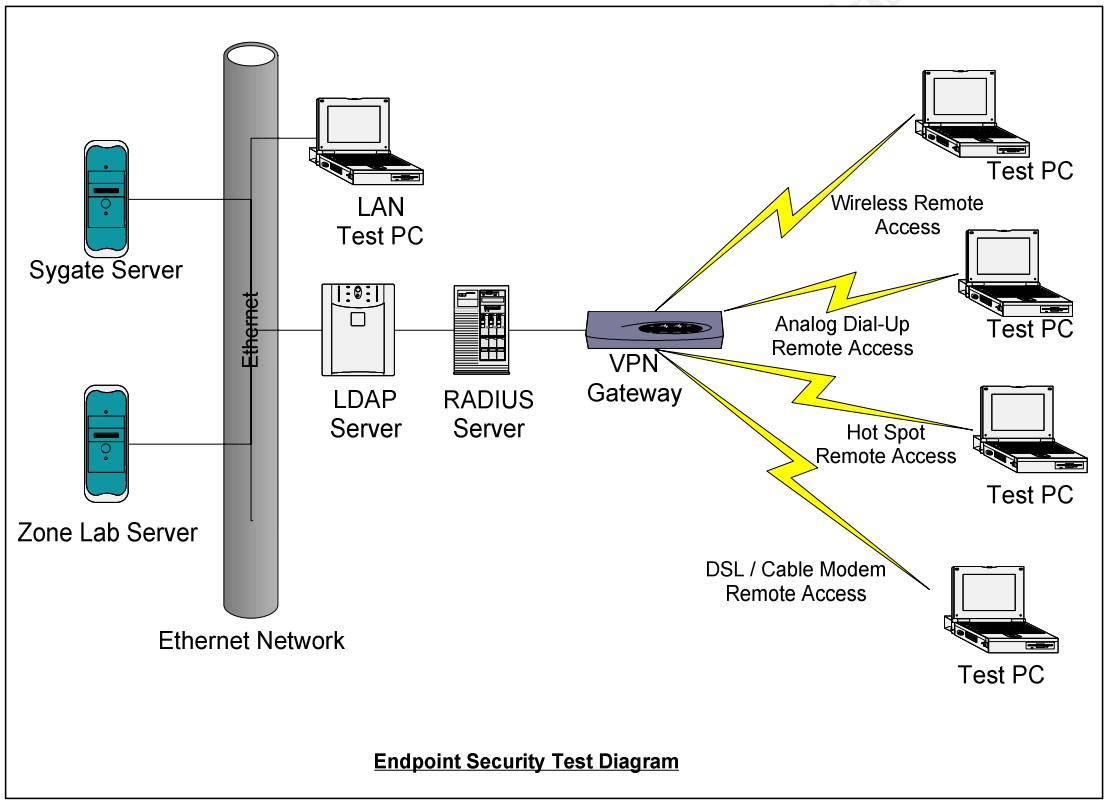
- Impact or disruption to users?
- Project plan needs to be created.
- Can user circumvent the endpoint solution?
- Installation Automatic?

[22] Cisco Systems, Inc.. Security At The Endpoint: Cisco Acquires Okena. 1992-2004 Cisco VP Richard Palmer Explains How The Company's Latest Acquisition Will Help Customers Recognize And Defend Against Hostile Cyber Behavior. 12 July 2004. <http://newsroom.cisco.com/dlls/hd_012403.html>.

- How does the endpoint security solution improve security rating?
- What gets checked or verified?
- Do the products disallow port or Ip address scanning, like anti-spoofing at endpoint systems?
- Can we set up remediation to occur automatically?
- What's the solution diagram look like?
- What if the server or enforcer is down, will laptops agents still be operational and / or enforcing security policy?
- What are the server manager redundant set-up requirements?
- Content filter capable? Example, can the software prevent access to certain web sites (like xxx.com?)

Evaluation and Pilot Set-Up

The following evaluation diagram was used for testing.



Endpoint Security Test Diagram

Endpoint client agents are installed in test personal computers (Test PCs). Test PCs can be desktops, laptops, or servers. Policy management software is

installed on the Sygate and Zone Lab servers. Policy enforcement point or enforcer is at the VPN gateway. Enforcers communicate with policy server to obtain security policies and agent authentication information. The enforcer can be any network entry points such as VPN, Wireless AP, RAS dial-up servers, or at key points on internal LAN devices like laptops, desktops, or servers. Almost anything that communicates 802.1 x protocols can be an enforcer.

Sygate

Sygate's endpoint security product is called Secure Enterprise. This solution uses a layered security approach that includes both Signature-based and Behavioral-based (or Application-based) analysis as a host based intrusion detection system. In a signature-based scenario, the application looks for possible intrusions by monitoring system log files, kernel log files, critical system files and other known attacks. Signature-based detection method is based on a list of known attacks, called signature lists. Signature-based detection is reactive in nature because it has to check against a list of signatures. The behavioral-based is often referred to as Application-based analysis because it seeks anomaly in the application behavior to determine an attack. If an intrusion is detected, the software can be set up to generate an alert or take action such as execute a file or restore systems files.

The Sygate Secure Enterprise product uses a third layer called Host Integrity. The Host Integrity is heart of the product. It automatically enforces and remediates the security policy of the endpoint before allowing network access.

Sygate Evaluation Process

Sygate evaluation process starts by entering in a nondisclosure agreement (NDA). After completing this form, you are entered in their system and an evaluation license is generated. Their SE is usually open to come out to help or train you on how to use their software. Also, access to their Enterprise Support team for assistance is available. I found the best way to get familiar with their product is through product literatures like users and installation guides.

Sygate Evaluation and Pilot Findings

The product supports most network access systems (NAS) vendors like Checkpoint, Cisco, and Nortel Network. In the evaluation diagram, the VPN gateway is a NAS device. The implementation process is simply to build the

agents and deploy out using CD, Microsoft SMS, or using a managing server or some web server and get users to point to that link for agent download.

My recommendation on piloting is to use three percent trial on IT folks and perform due diligent. After that, give 2 weeks to implement. Sygate management server installation is pretty much automatic. The whole process took about 20 minutes to load. An important option is to choose mix mode authentication for SQL server. For the user agent installs, use SMS to download the agent. Then reboot the client machines for the software to take affect.

The agent takes between 3 to 5% performance hit on laptops and personal computers. The agents can be deployed in silent mode or it can show on the computer tray for users to see. Remediation depends on how the policy is configured; automatically in inside web server or to window's update.com. You can even setup to re-route users to a web server or have a POP up window saying 'you failed host integrity.'

Sygate can check for any process, application, registry entry, or services running, any file as long as you have the path. It can regulate Instant Messenger applications also. I loaded Yahoo IM and was able to control the access to virtually any application on the host machine.

Sygate Evaluation and Pilot Conclusion

I found Sygate's management interface to be extremely user friendly. I was able to test most of the required features successfully. However, I discovered that there is a way users can circumvent the solution. In a DOS command line, entering the 'netstop smc service' command turns off the Sygate agent, even if that option is disallowed in the security policy by the administrator. Needless to say, I immediately consulted with Sygate. They confirmed that this is the case in version 3.5 and before (I was testing with Sygate version 3.5). They claimed that this is not a bug but in fact a feature; Users can SMC start or stop to stop the agent. Due to user's request to disable this ability, they are releasing version 4.0. Version 4.0 password protects the endpoint devices where users can not turn off the agent. In this new version, running the command 'netstop smc service' will be prompted for a password. Without knowing the disabling password, agents can not be disabled.

Zone Labs

The Zone Labs endpoint security server is called Integrity Server. This is an independent management server that comes with a build in database; though a

3rd party database like Microsoft SQL can be used. At the time of evaluation, Integrity version 4.5 was available. This version works with 802.1x compatible devices, just like Sygate.

The Integrity Gateway is a Server Application residing on NAS gateway or Integrity Server for enforcement. It enforces policies and performs checks and verifications before allowing access to network (just like the enforcement device for a Sygate). The functions of the Integrity Gateway are to:

- Verify integrity client is running on endpoint computer.
- Verify client policies are up-to-date (by pre-configuring client policies with firewall, application control, ports and application allowed or deny, and other security setting).
- Prevent non-complaint computers from accessing network.
- Prevent client from shutting down the agent by using their TrueVector Security engine after logging in; therefore, it maintains security while client is logged on to the network.

Integrity Gateway is supported for the following products:

- Nortel Contivity with Tunnel Guard – Firmware version 4.80 or above
- Cisco 3000 VPN
- Checkpoint VPN-1 Secure Client and Firewall-1 using secure configuration verification (SCV)
- Cisco Wireless Access Point 1100 – An 802.1x compatible device
- Microsoft RAS Server 2003

The Integrity Client or Application Agent resides on endpoint computers. The agent consists of these three features or configuration options. Integrity Agent is for non-security aware users or general users. Basically, users will have no control over policy on their client system. The Integrity Flex is for security aware users. This option allows users to configure their own policy. The third option is Integrity Desktop for non-laptop devices or workstations in the company facility.

The enforcement checks that Integrity agent exists and verifies against security policy. The enforcement terminates network access if any of the previous two is not met. Endpoint computer has specific setting and security policies configured. After login to the network, the user is prevented from disabling the security agent.

There are 2 security models to choose from in Zone Labs. An IP based model is where security is based on machine IP address. A user based model security is on authorized user account, like Login ID.

A user based model is also referred to Authentication based security model. This security model is most beneficial where endpoint systems are used by more than

one user. This model provides higher level of security. User accounts or groups are required to be set up on NT Domain, RADIUS, and Active Directory or on any LDAP for the Zone Labs server to link up to it.

A benefit of an IP based model is that it is quicker to deploy. Most companies start with IP based and then switch to User based. Also, combination of IP based and User based model can be used. In this scenario, the Zone Labs sever will put priorities like a user based has higher priority than IP based.

Zone Labs Evaluation Process

Zone Labs evaluation process is similar to the Sygate process. It starts by entering in a nondisclosure agreement (NDA). Then an evaluation license is generated and you can download the software from Zone Labs website. Use the evaluation license to complete the evaluation installation. Their SE was extremely helpful and guided me through the installation process.

Zone Labs Evaluation and Pilot Findings

For the client deployment options, they include distributing the agent software in a Sandbox (like a web server) where users can go there for support information, download and extract (self) the packages; distribute the software and documentation in a CD; or Microsoft SMS to roll the agents out. Once the agents are deployed, upgrades can be seamless with policy push or enforcement. You can set up the policy to have a 'POP' up window for non-compliant versions. If you're using a Sandbox, on the POP up window, a link can be provided to direct users to go to for remediation. This remediation process can also be automatic where Agent can be silently installed or can be on the tray. Currently, Zone Labs support Windows clients only.

The impact can be extremely minimal if you want to observe and run silently. Generally, the more secure your environment and the more strictly you enforce specific settings, the higher the user impact. The installation is pretty automatic at the server end. It took 15 to 30 minutes to complete the server installation. At the client end, installation can be performed silently to minimize user impact. It can also be user aware during this process.

A list of check and verification capabilities performed is:

- Registry (specific setting or "not empty").

- File: existence, state (running?), version range, modified date age, and/or match smart checksum of a reference file.
- Anti-virus (any one of 5 major providers): minimum engine version, state (running?), and/or maximum age of anti-virus software.
- Anti-Virus DAT age limit, minimum version, or last download date.

For the above two tests, endpoints were tested to be required to be in compliance. If not, network access is disallowed.

At first, I was not able to test successfully the following:

1. File checking – joe.wri file checking was not successful
2. Deny access - Deny pings to the Integrity Server were not successful when client does not comply.
3. VPN Gateway to Client communication - Tunnel Guard client was not communicating with VPN Gateway successfully according to VPN Gateway.
4. Clear VPN Gateway Errors - Error messages on VPN Gateway are, "Restricted filter no longer required. Restoring initial filter permit all"

After some troubleshooting with the VPN Gateway vendor, I discovered that we had a bad Ethernet card. After getting that resolved, these tests came out clean.

Zone Evaluation Conclusion

The management interface was not as user friendly as Sygate's. I imagine Zone Lab's management interface will change to a more Checkpoint management interface look and feel. The management interface should not be a problem in the future since I currently manage the Checkpoint Firewall.

All the required features tested fine. I could not find a way to circumvent the solution. The agent on the test systems were not able to be turned off if the policy disallows it.

Overall Evaluation and Pilot Result

Below is the evaluation and pilot result.

Evaluation Result			
Order	**Evaluation Criteria**	**Sygate**	**Zone Labs**
1	Ability to manage anti-virus on computer workstations and laptops.	Yes	Yes
2	Ability to certify anti-virus software while connecting to the network.	Yes	Yes
3	Ability to ensure that anti-virus is updated.	Yes	Yes
4	Restrict users from accessing the company network resources from unauthorized computers.	Yes	Yes
5	Users can not circumvent solution.	No	Yes
6	Secure end devices against port scans, malicious code injections and other cyber attacks while accessing from home or at public wireless networks, like hotspots.	Yes	Yes
7	Ensure security and integrity of Wireless Local Area Networks, PDAs, Wireless Hotspots, and Instant Messaging medium accesses.	Yes	Yes

Having an endpoint security mechanism will improve the security of Remote Access VPN communication. Overall Remote Access Users security rating will improve from 2.875 to 4.5 with endpoint security. Wireless Hotspot is and will remain one of the weakest security areas. This is because of the nature of this architecture. Wireless Hotspots are wireless communications originated at public wireless centers; like Starbucks, McDonald's, Airports, etc.. Because it is a public infrastructure, these connections are more susceptible to security risks. Implementing endpoint security will improve this security rating and lower threats to user systems and to our corporate network. We can not influence or have complete control over the Wireless Hotspot security infrastructure; we are arm only with endpoint security mitigation techniques.

Recommendation

Zone Labs does not rely on signature updates unlike Anti-Virus software and Intrusion Detection and Prevention systems do. Instead it relies on Application control and sophisticated projection at the Network protocol layer to neutralize threats. It protects against malware, port scanning, denial-of-service attacks, Trojan horses, and malicious codes. Sygate on the other hand has the additional Intrusion Detection and Prevention functionality.

For our environment, Zone Labs has an upper edge. Feature wise, Sygate and Zone Labs are neck to neck. We are using Checkpoint Firewall and since they just acquired Zone Labs, we will have centralized management for both Corporate Firewall and Endpoint Security without compromising endpoint features. Also, I was able to circumvent the Sygate agent with the version 3.5 during the evaluation.

Deployment

Unfortunately, this document has to be submitted before the completion of the initial deployment. I can however write about the deployment game plan.

Architecturally, the Integrity Server will be set-up to operate in fail-over mode for redundancy. One server will function as primary in active state while the other will be secondary in passive state. The pilot and initial deployment will be broken down to three phases. The infrastructure implementation phase should have no users' impact. Users continue using existing remote access VPN solution during this phase. The installation of the Integrity Server and configuring it to function with the LDAP and VPN Gateway are part of this phase. The next phase is to pilot with a few users (non IT staffs). General users will have no impact in this phase as they will continue using existing remote access VPN solution. In this phase, most IT administrators will be selected to deploy Endpoint clients in their laptops. The final phase is the roll out, which includes initial general users' deployment. I plan to use Microsoft's SMS to deploy client agents in silent mode. Initially low security regulation will be turned on. This is so users will get comfortable with this new agent in their computers. The plan is to slowly increase security restriction afterwards. For maintenance and support, users will be instructed to call into Helpdesk. FAQ, troubleshooting tips, and other communication documentations will be posted on-line. I imagine the deployment process will be straightforward since due diligence was performed in the evaluation pilot phase. Fine-tuning and enforcing endpoint security policy will take time and will be a manual process.

Conclusion

The traditional perimeter security solution is not enough to protect corporate asset and data. Network access has expanded from origination within business facility, where physical security and network transport medium are more certain – At which they are controlled and or managed by a company, to any where any time over any network medium access. Corporate users can access company data and resources at home, at wireless hotspots, or at anywhere outside the

confines of corporate facilities. The ubiquity of network access makes the traditional perimeter security solution not adequate to secure company asset and data and to protect them against hackers, unauthorized accesses, and malicious code and virus injections. The solution is to expand the network perimeter to end systems with an Endpoint Security solution.

Appendix A. Glossary

Checkpoint Stateful Inspection: Stateful Inspection, invented and patented by Check Point, is the de facto standard in network security technology. Stateful Inspection provides accurate and highly efficient traffic inspection with full application-layer awareness for the highest level of security.[23]

Cisco PIX Security Appliance: Cisco PIX Security Appliances provide robust, enterprise-class integrated network security services to create a strong multilayered defense for fast-changing network environments.[24]

Demilitarized zone (DMZ): An area from which military forces, operations, and installations are prohibited.[25]

Enhanced IGRP (EIGRP): Enhanced IGRP provides compatibility and seamless interoperation with IGRP routers. An automatic-redistribution mechanism allows IGRP routes to be imported into Enhanced IGRP, and vice versa, so it is possible to add Enhanced IGRP gradually into an existing IGRP network.[26]

Flapping: A condition where a service is up and down repeatedly.

Generic Routing Encapsulation (GRE): Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.[27]

Institute of Electrical Engineers (IEEE): From its earliest origins, the IEEE has advanced the theory and application of electro technology and allied sciences, served as a catalyst for technological innovation and supported the needs of its members through a wide variety of programs and services.[28]

---

[23] Check Point Software Tchnologies, Ltd.. Stateful Technologies description. 12 July 2004. <http://www.checkpoint.com/products/technologies/stateful_inspect.html>.
[24] Cisco Systems, Inc.. 1992-2004 Cisco PIX Security Appliances Product Introduction. 12 July 2004. <http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html>.
[25] Dictionary.com. Lexico Publishing Group, LLC. 2004. DMZ Definition. 12 July 2004. <http://dictionary.reference.com/search?q=DMZ>.
[26] Cisco Systems, Inc.. 1992-2004. EIGRP Introduction. 12 July 2004. <http://www.cisco.com/en/US/tech/tk365/tk207/tech_protocol_family_home.html>.
[27] Cisco Systems, Inc.. 1992-2004. GRE Introduction. 12 July 2004. <http://www.cisco.com/en/US/tech/tk827/tk369/tk287/tech_protocol_home.html>.
[28] Institute of Electrical and Electronics Engineers, Inc. 2004. About IEEE. 12 July 2004. <http://www.ieee.org/portal/index.jsp?pageID=corp_level1&path=about/whatis&file=index.xml&xsl=generic.xsl>.

Integrated Services Digital Network (ISDN): Is a system of digital phone connections which has been available for over a decade. This system allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity.[29]

IP Secure (IPSec): A protocol that provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating devices.[30]

Mean-Time-To-Recovery (MTTR): The average time that a device will take to recover from a non-terminal failure.[31]

Nokia VRRP: The Virtual Router Redundancy Protocol (VRRP) enables implementation of hot-standby firewall appliances in a way that is transparent to host systems. Hosts are able to utilize a hot-standby firewall appliance if the primary appliance fails - without the need for any direct host involvement. By combining VRRP with Check Point Firewall Sync, Nokia firewall appliances can be deployed in configurations that support integrated, redundant, hot-standby routing and firewall services.[32]

Out-Of-Band-Management (OOB): Management scheme that does not use the same communication path between the managing devices and the managed elements.[33]

Return-On-Investment (ROI): A measure of the net income a firm's management is able to earn with its total assets. Return on investment is calculated by dividing net profits after taxes by total assets.[34]

SPAM: Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.[35]

---

[29] Ralphb.net. Ralph Becker, 4 December 2003. ISDN Tutorial. 12 July 2004. <http://www.ralphb.net/ISDN/defs.html>.
[30] Dictionary.com. Lexico Publishing Group, LLC. 2004. IPSec Definition. 12 July 2004. <http://dictionary.reference.com/search?q=IPSec>.
[31] Dictionary.com. Lexico Publishing Group, LLC. 2004. MTTR Definition. 12 July 2004. <http://dictionary.reference.com/search?q=mean%20time%20to%20recovery>.
[32] Nokia. 2004. VRRP Firewall Sync Key Benefits. 12 July 2004. <http://www.nokia.com/nokia/0,,3321,00.html>.
[33] TECSys Development, Inc.. Darel Stokes. 9 April 2002. Out-Of-Band Management in the Enterprise. 12 July 2004. <http://www.tditx.com/pdf/03_Out-Of-Band_Management_Enterprise_09-04-2002.pdf>.
[34] Dictionary.com. Lexico Publishing Group, LLC. 2004. ROI Definition. 12 July 2004. <http://dictionary.reference.com/search?r=2&q=return%20on%20investment%20%20ROI%20>.
[35] Dictionary.com. Lexico Publishing Group, LLC. 2004. SPAM Definition. 12 July 2004. <http://dictionary.reference.com/search?q=SPAM>.

Split Tunnel: Allowing tunnel endpoints to continue using its existing Internet connection for non-VPN related traffic rather than through the IPSec tunnel.[36]

Virtual Private Network (VPN): The use of encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.[37]

[36] Cisco Systems, Inc.. 1992-2004. Design Guide. Planning Issues and Decisions. 12 July 2004. <http://www.cisco.com/en/US/netsol/ns341/ns396/ns172/ns334/networking_solutions_design_guide_chapter09186a008017e6c6.html>.
[37] Dictionary.com. Lexico Publishing Group, LLC. 2004. VPN Definition. 12 July 2004. <http://dictionary.reference.com/search?q=virtual%20private%20network>.

Appendix B. Reference List

References

Trend Micro Incorporated. InterScan VirusWall Product Overview. 28 June 2004 <http://www.trendmicro.com/en/products/gateway/isvw/evaluate/overview.htm>.

Trend Micro Incorporated. InterScan VirusWall Features. 28 June 2004 <http://www.trendmicro.com/en/products/gateway/isvw/evaluate/features.htm>.

Check Point Software Technologies Ltd.. October 5, 1998. Check Point Software Technologies And Trend Micro Team To Combat Internet Gateway Security Threats. 28 June 2004 <http://www.checkpoint.com/press/1998/trendmicro100598.html>.

IntelliReach Corporation Website. Email Management Solutions. 28 June 2004. <http://www.intellireach.com/index.htm>.

IntilleReach Corporation. The MessageScreen Advantage. 28 June 2004 <http://www.intellireach.com/products/messagescreen/MS_advantage.htm>.

IntilleReach Corporation. MessageScreen Product Description. 28 June 2004 <http://www.intellireach.com/products/messagescreen/index.htm>.

IntilleReach Corporation. The MessageScreen Advantage. 2 July 2004. <http://www.intellireach.com/products/messagescreen/MS_advantage.htm>.

The SANS™ Institute. The SANS Security Policy Project. 2002-2004. Need an Example Policy or Template? 2 July 2004. <http://www.sans.org/resources/policies/>.

The SANS™ Institute. The SANS Security Policy Project. 2002-2004. Is it a Policy, a Standard or a Guideline? 6 July 2004. <http://www.sans.org/resources/policies/>.

Internet Security Systems. Proventia Intrusion Prevention Product Overview. 8 July 2004. <http://www.iss.net/products_services/enterprise_protection/proventia/g_series.php>.

NetIQ Corporation. 1993 – 2004. Security Management Solution Overview. 8 July 2004. <http://www.netiq.com/solutions/security/default.asp>.

CSO online.com. Michael Rasmussen, Forrester®. 2004. Demand for Endpoint Security Growing. 6 July 2004 <http://www.csoonline.com/analyst/report2170.html>.

RSA Conference Portal. Conference Portal website. 9 July 2004. <http://www.rsaconference.com/conf_portal.html>.

Network World Fusion. Company website. 9 July 2004. <http://www.nwfusion.com/>.

Google Search Engine. 2004 Google. Search Engine portal. 10 July 2004. <http://www.google.com/search?hl=en&ie=UTF-8&q=endpoint+security>.

Check Point Software Technologies, Ltd.. Endpoint security solution. VPN-1 Secure Client. 10 July 2004. <http://www.checkpoint.com/products/vpn-1_clients/index.html>.

Cisco Systems, Inc.. 1992-2004 Cisco Security Agent Introduction. 10 July 2004. <http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html>.

Sygate Inc.. 2004. Sygate Secure Enterprise. 10 July 2004. <http://www.sygate.com/products/sygate-secure-enterprise.htm>.

Zone Labs Inc.. 1999 – 2004. Zone Labs Integrity Enterprise Endpoint Security. 10 July 2004. <http://www.zonelabs.com/store/content/company/corpsales/intOverview.jsp;jsessionid=As1jI5ThbQawT6VgDhtjAcq2mk25pvAQk8qNFu3e11YsHCfabErE!-30283316!-1062696905!7551!7552!-2012896460!-1062696904!7551!7552>.

Microsoft Corporation. 2004. MSDN Library. 11 July 2004. <http://msdn.microsoft.com/library/default.asp?url=/downloads/list/webdev.asp>.

Network World Fusion. Tim Greene, IDG News Service, 15 December 2003. Check Point buys Zone to bolster endpoint security. 11 July 2004. <http://www.nwfusion.com/net.worker/news/2003/1215checkzone.html>.

Cisco Systems, Inc.. Security At The Endpoint: Cisco Acquires Okena. 1992-2004 Cisco VP Richard Palmer Explains How The Company's Latest Acquisition Will Help Customers Recognize And Defend Against Hostile Cyber Behavior. 12 July 2004. <http://newsroom.cisco.com/dlls/hd_012403.html>.

Check Point Software Tchnologies, Ltd.. Stateful Technologies description. 12 July 2004. <http://www.checkpoint.com/products/technologies/stateful_inspect.html>.

Cisco Systems, Inc.. 1992-2004 Cisco PIX Security Appliances Product Introduction. 12 July 2004. <http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html>.

Dictionary.com. Lexico Publishing Group, LLC. 2004. DMZ Definition. 12 July 2004. <http://dictionary.reference.com/search?q=DMZ>.

Cisco Systems, Inc.. 1992-2004. EIGRP Introduction. 12 July 2004. <http://www.cisco.com/en/US/tech/tk365/tk207/tech_protocol_family_home.html> .

Cisco Systems, Inc.. 1992-2004. GRE Introduction. 12 July 2004. <http://www.cisco.com/en/US/tech/tk827/tk369/tk287/tech_protocol_home.html>.

Institute of Electrical and Electronics Engineers, Inc. 2004. About IEEE. 12 July 2004. <http://www.ieee.org/portal/index.jsp?pageID=corp_level1&path=about/whatis&file=index.xml&xsl=generic.xsl>.

Ralphb.net. Ralph Becker, 4 December 2003. ISDN Tutorial. 12 July 2004. <http://www.ralphb.net/ISDN/defs.html>.

Dictionary.com. Lexico Publishing Group, LLC. 2004. IPSec Definition. 12 July 2004. <http://dictionary.reference.com/search?q=IPSec>.

Dictionary.com. Lexico Publishing Group, LLC. 2004. MTTR Definition. 12 July 2004. <http://dictionary.reference.com/search?q=mean%20time%20to%20recovery>.

Nokia. 2004. VRRP Firewall Sync Key Benefits. 12 July 2004. <http://www.nokia.com/nokia/0,,3321,00.html>.

TECSys Development, Inc.. Darel Stokes. 9 April 2002. Out-Of-Band Management in the Enterprise. 12 July 2004. <http://www.tditx.com/pdf/03_Out-Of-Band_Management_Enterprise_09-04-2002.pdf>.

Dictionary.com. Lexico Publishing Group, LLC. 2004. ROI Definition. 12 July 2004. <http://dictionary.reference.com/search?r=2&q=return%20on%20investment%20%20ROI%20>.

Dictionary.com. Lexico Publishing Group, LLC. 2004. SPAM Definition. 12 July 2004. <http://dictionary.reference.com/search?q=SPAM>.

Cisco Systems, Inc.. 1992-2004. Design Guide. Planning Issues and Decisions. 12 July 2004.

<http://www.cisco.com/en/US/netsol/ns341/ns396/ns172/ns334/networking_solutions_design_guide_chapter09186a008017e6c6.html>.

Dictionary.com. Lexico Publishing Group, LLC. 2004. VPN Definition. 12 July 2004. <http://dictionary.reference.com/search?q=virtual%20private%20network>.

Last Updated: May 25th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced